



# Sophos Anti-Virus for Linux user manual

Product version: 7

Document date: January 2011



# Contents

|  |    |
|--|----|
| 1 About this manual.....                           | 3  |
| 2 About Sophos Anti-Virus for Linux.....           | 4  |
| 3 On-access scanning.....                          | 7  |
| 4 On-demand scanning.....                          | 10 |
| 5 What happens if viruses are detected.....        | 14 |
| 6 Cleaning up viruses.....                         | 16 |
| 7 View the Sophos Anti-Virus log.....              | 19 |
| 8 Update Sophos Anti-Virus immediately.....        | 20 |
| 9 About kernel support.....                        | 21 |
| 10 Configure the web UI.....                       | 22 |
| 11 Appendix A: On-demand scan return codes.....    | 23 |
| 12 Appendix B: About CID-based configuration.....  | 25 |
| 13 Appendix C: Configuring scheduled scans.....    | 30 |
| 14 Appendix D: Configuring alerts.....             | 34 |
| 15 Appendix E: Configure logging.....              | 40 |
| 16 Appendix F: Configuring updating.....           | 41 |
| 17 Appendix G: Configuring on-access scanning..... | 46 |
| 18 Troubleshooting.....                            | 51 |
| 19 Glossary.....                                   | 56 |
| 20 Technical support.....                          | 58 |
| 21 Legal notices.....                              | 59 |

# 1 About this manual

This manual tells you how to use and configure Sophos Anti-Virus for Linux.

To install or uninstall Sophos Anti-Virus on networked and single Linux computers, see the *Sophos Anti-Virus for Linux startup guide* for version 7.

To install Sophos Anti-Virus on a mixed Linux and Windows network, or to centrally manage Sophos Anti-Virus using Sophos Enterprise Console, see the *Sophos Endpoint Security and Control startup guide for Linux, NetWare, and UNIX*.

Sophos documentation is published at [www.sophos.com/support/docs/](http://www.sophos.com/support/docs/).

## 2 About Sophos Anti-Virus for Linux

### 2.1 What Sophos Anti-Virus does

Sophos Anti-Virus detects and deals with viruses (including worms and Trojans) on your Linux computer. As well as being able to detect all Linux viruses, it can also detect all non-Linux viruses that might be stored on your Linux computer and transferred to non-Linux computers. It does this by scanning your computer.

### 2.2 How Sophos Anti-Virus protects your computer

*On-access scanning* is your main method of protection against viruses. Whenever you access (copy, save, or open) a file, Sophos Anti-Virus scans the file and grants access to it only if it does not pose a threat to your computer.

In addition to on-access scanning, Sophos Anti-Virus enables you to run an *on-demand scan* to provide additional protection. An on-demand scan is a scan that you initiate. You can scan anything from a single file to everything on your computer that you have permission to read. You can either manually run an on-demand scan or schedule it to run unattended.

### 2.3 How you use Sophos Anti-Virus

Sophos Anti-Virus has two types of user interface:

- Command-line interface (CLI)
- Web user interface (web UI)

Use the interface that you prefer but note that you can use the web UI to perform only certain tasks, listed below.

For tasks that you can perform using either interface, this document explains both methods, in subsections headed either *CLI* or *Web UI*, respectively.

#### 2.3.1 Command-line interface (CLI)

The command-line interface enables you to perform all tasks. It is the only way to run on-demand scans and configure updating.

**Note:** You must be logged on to the computer as root to use all commands except **savscan**, which is used to run on-demand scans.

This document assumes that you have installed Sophos Anti-Virus in the default location, `/opt/sophos-av`. The paths of the commands described are based on this location.

## 2.3.2 Web user interface (web UI)

The web user interface enables you to:

- Check that on-access scanning is active.
- Start and stop on-access scanning.
- Configure on-access scanning inside archives.
- Configure what is excluded from on-access scanning.
- Configure alerts.
- View the Sophos Anti-Virus log.
- Configure on-access cleanup.

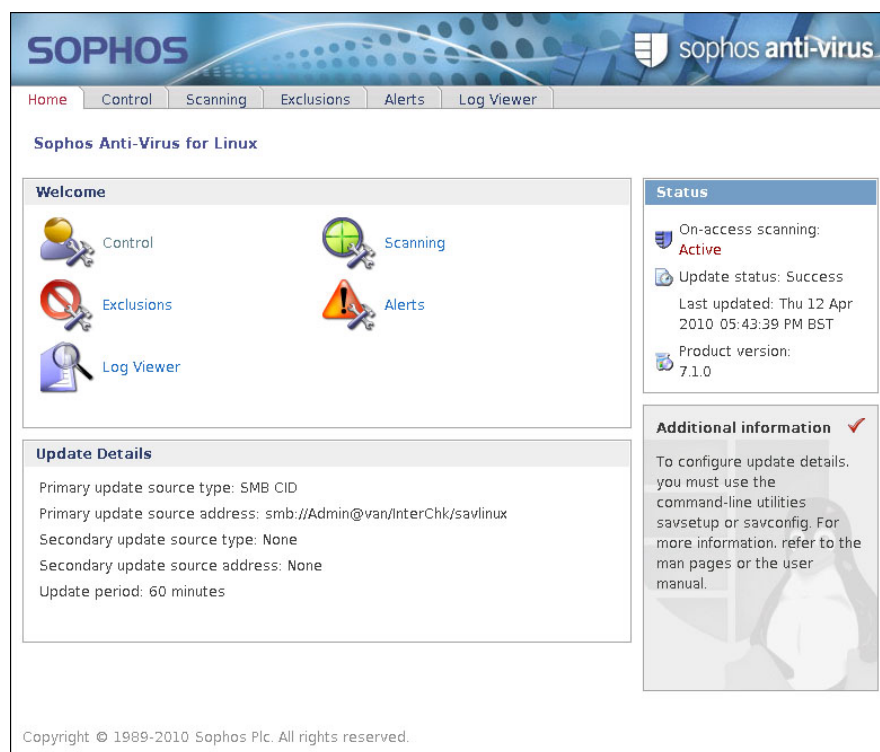
To run on-demand scans and configure updating, you must use the CLI.

**Note:** Although the web UI can be run by the root user (as well as other users), it does not run with root privileges. It cannot therefore access all files on the computer.

### To use the web UI

1. Point a web browser to **http://localhost:8081**.

The browser displays the **Home** tab of the web UI.



2. When you click another tab, the browser asks you for credentials so that you can use the web UI to configure Sophos Anti-Virus.

To find out your username, either ask your system administrator or, at a command prompt, type:

```
/opt/sophos-av/bin/savconfig query HttpUsername
```

**Note:** To find out your username in this way, you must be logged on to the computer as root.

To find out your password, ask your system administrator.

## 2.4 How you configure Sophos Anti-Virus

If your Linux computers are managed by Sophos Enterprise Console, configure Sophos Anti-Virus as follows:

- Configure **on-access scanning, scheduled scans, alerting, logging, and updating** centrally from Enterprise Console. For information, see the Enterprise Console Help.

**Note:** These features also include some parameters that cannot be set using Enterprise Console. You can set these parameters from the Sophos Anti-Virus CLI on each Linux computer locally. Enterprise Console ignores them.

- Configure **on-demand scans and the web user interface** from the Sophos Anti-Virus CLI on each Linux computer locally.

If you have a network of Linux computers that is *not* managed by Enterprise Console, configure Sophos Anti-Virus as follows:

- Configure **on-access scanning, scheduled scans, alerting, logging, updating, and the web user interface** centrally by editing a configuration file in the central installation directory (CID) from which the computers update. This is called CID-based configuration.

- Configure **on-demand scans** from the Sophos Anti-Virus CLI on each computer locally.

**Note:** Do not use CID-based configuration unless technical support advises you to do so, or you cannot use Enterprise Console. You cannot use Enterprise Console configuration and CID-based configuration together.

If you have a standalone Linux computer that is *not* managed by Enterprise Console, configure Sophos Anti-Virus as follows:

- Configure **on-access scanning, scheduled scans, alerting, logging, updating, and the web user interface** from the Sophos Anti-Virus CLI or web UI.
- Configure **on-demand scans** from the Sophos Anti-Virus CLI.

## 3 On-access scanning

*On-access scanning* is your main method of protection against viruses. Whenever you access (copy, save, or open) a file, Sophos Anti-Virus scans the file and grants access to it only if it does not pose a threat to your computer.

### 3.1 Check that on-access scanning is active

#### 3.1.1 CLI

- To check that on-access scanning is active, type:  
`/opt/sophos-av/bin/savdstatus`

#### 3.1.2 Web UI

- To check that on-access scanning is active, look at the **Status** panel.

### 3.2 Check on-access scanning will be started automatically on system boot

#### 3.2.1 CLI

To perform this procedure, you must be logged on to the computer as root.

1. Check that **savd** will be started automatically on system boot:  
`chkconfig --list`

**Note:** If this command does not work on your Linux distribution, use the appropriate utility to display services that are configured to start on system boot.

If the list contains an entry for sav-protect with 2:on, 3:on, 4:on and 5:on, on-access scanning will be started automatically on system boot.

Otherwise, type:

`/opt/sophos-av/bin/savdctl enableOnBoot savd`

2. Check that on-access scanning will be started automatically with **savd**:

**/opt/sophos-av/bin/savconfig query EnableOnStart**

If the command returns `true`, on-access scanning will be started automatically with **savd** on system boot.

Otherwise, type:

**/opt/sophos-av/bin/savconfig set EnableOnStart true**

### 3.2.2 Web UI

- To check on-access scanning will be started automatically on system boot, on the **Control** tab, check the **Startup** panel.

If the **Start on-access scanning on system boot** check box is selected, on-access scanning will be started automatically on system boot.

## 3.3 Start on-access scanning

### 3.3.1 CLI

To start on-access scanning, do one of the following:

- Type:

**/opt/sophos-av/bin/savdctl enable**

- Use the appropriate tool to start the installed service `sav-protect`. For example, type:

**/etc/init.d/sav-protect start**

or

**service sav-protect start**

### 3.3.2 Web UI

- To start on-access scanning, on the **Control** tab, in the **Control** panel, click **Enable On-access Scanning**.

## 3.4 Stop on-access scanning

**Important:** If you stop on-access scanning, Sophos Anti-Virus does not scan files that you access for viruses. This puts your computer, and others to which it is connected, at risk.



### 3.4.1 CLI

- To stop on-access scanning, type:  
`/opt/sophos-av/bin/savdctl disable`

### 3.4.2 Web UI

- To stop on-access scanning, on the **Control** tab, in the **Control** panel, click **Disable On-access Scanning**.

## 4 On-demand scanning

An *on-demand scan* is a scan that you initiate. You can scan anything from a single file to everything on your computer that you have permission to read. You can either manually run an on-demand scan or schedule it to run unattended.

To schedule an on-demand scan, see [Appendix C: Configuring scheduled scans](#).

### 4.1 Running on-demand scans

The command that you type to run an on-demand scan is **savscan**.

#### 4.1.1 Scan the computer

- To scan the computer, type:  
**savscan /**

**Note:** You can also use Sophos Enterprise Console to run a full scan on one or more computers. For details, see the Enterprise Console Help.

#### 4.1.2 Scan a particular directory or file

- To scan a particular directory or file, specify the path of the item. For example, type:  
**savscan /usr/mydirectory/myfile**

You can type more than one directory or file in the same command.

#### 4.1.3 Scan a filesystem

- To scan a filesystem, specify its name. For example, type:  
**savscan /home**

You can type more than one filesystem in the same command.

#### 4.1.4 Scan a boot sector

To scan a boot sector, log in as superuser. This grants you sufficient permission to access the disk devices.

You can scan the boot sector of a logical or physical drive.

- To scan the boot sector of specific logical drives, type:  
**savscan -bs=drive, drive, ...**

where *drive* is the name of a drive, for example `/dev/fd0` or `/dev/hda1`.

- To scan the boot sector of all logical drives that Sophos Anti-Virus recognises, type:  
**savscan -bs**
- To scan the master boot record of all fixed physical drives on the computer, type:  
**savscan -mbr**

## 4.2 Configuring on-demand scans

In this section, where *path* appears in a command, it refers to the path to be scanned.

To see a full list of the options that you can use with an on-demand scan, type:

**man savscan**

### 4.2.1 Scan all file types

By default, Sophos Anti-Virus scans only executables. To see a full list of the file types that Sophos Anti-Virus scans by default, type **savscan -vv**.

- To scan all file types, not just those that are scanned by default, use the option **-all**. Type:  
**savscan path -all**

**Note:** This makes scanning take longer, can compromise performance on servers, and can cause false virus reports.

### 4.2.2 Scan a particular file type

By default, Sophos Anti-Virus scans only executables. To see a full list of the file types that Sophos Anti-Virus scans by default, type **savscan -vv**.

- To scan a particular file type, use the option **-ext** with the appropriate filename extension. For example, to scan files that have the filename extension `.txt`, type:  
**savscan path -ext=txt**
- To disable scanning of a particular file type, use the option **-next** with the appropriate filename extension.

**Note:** To specify more than one file type, separate each filename extension with a comma.

### 4.2.3 Scan inside all archive types

You can configure Sophos Anti-Virus to scan inside all archive types. To see a list of these archive types, type **savscan -vv**.

- To scan inside all archive types, use the option **-archive**. Type:

#### **savscan path -archive**

Archives that are “nested” within other archives (for example, a TAR archive within a ZIP archive) are scanned recursively.

If you have numerous complex archives, the scan may take longer to run. Bear this in mind when scheduling unattended scans.

### **4.2.4 Scan inside a particular archive type**

You can configure Sophos Anti-Virus to scan inside a particular archive type. To see a list of these archive types, type **savscan -vv**.

- To scan inside a particular archive type, use the option that is shown in the list. For example, to scan inside TAR and ZIP archives, type:

**savscan path -tar -zip**

Archives that are “nested” within other archives (for example, a TAR archive within a ZIP archive) are scanned recursively.

If you have numerous complex archives, the scan may take longer to run. Bear this in mind when scheduling unattended scans.

### **4.2.5 Scan remote computers**

By default, Sophos Anti-Virus does not scan items on remote computers (that is, does not traverse remote mount points).

- To scan remote computers, use the option **--no-stay-on-machine**. Type:

**savscan path --no-stay-on-machine**

### **4.2.6 Turn off scanning of symbolically linked items**

By default, Sophos Anti-Virus scans symbolically linked items.

- To turn off scanning of symbolically linked items, use the option **--no-follow-symlinks**. Type:  
**savscan path --no-follow-symlinks**

To avoid scanning items more than once, use the option **--backtrack-protection**.

### **4.2.7 Scan the starting filesystem only**

Sophos Anti-Virus can be configured not to scan items that are beyond the starting filesystem (that is, not to traverse mount points).

- To scan the starting filesystem only, use the option **--stay-on-filesystem**. Type:

**savscan path --stay-on-filesystem**

## 4.2.8 Excluding items from scanning

You can configure Sophos Anti-Virus to exclude particular items (files, directories, or filesystems) from scanning by using the option **-exclude**. Sophos Anti-Virus excludes any items that follow the option in the command string. For example, to scan items fred and harry, but not tom or peter, type:

**savscan fred harry -exclude tom peter**

You can exclude directories or files that are *under* a particular directory. For example, to scan all of Fred's home directory, but exclude the directory games (and all directories and files under it), type:

**savscan /home/fred -exclude /home/fred/games**

You can also configure Sophos Anti-Virus to *include* particular items that follow the option **-include**. For example, to scan items fred, harry, and bill, but not tom or peter, type:

**savscan fred harry -exclude tom peter -include bill**

## 4.2.9 Scan file types that UNIX defines as executables

By default, Sophos Anti-Virus does not scan file types that UNIX defines as executables.

- To scan file types that UNIX defines as executables, use the option **--examine-x-bit**. Type:  
**savscan path --examine-x-bit**

Sophos Anti-Virus still scans files that have filename extensions that are in its own list as well. To see a list of these filename extensions, type **savscan -vv**.

## 5 What happens if viruses are detected

Regardless of whether viruses are detected by on-access scanning or an on-demand scan, by default Sophos Anti-Virus:

- Logs the event in syslog and the Sophos Anti-Virus log (see [View the Sophos Anti-Virus log](#) (page 19)).
- Sends an alert to Enterprise Console if it is being managed by Enterprise Console.
- Sends an email alert to root@localhost.

By default, Sophos Anti-Virus also displays alerts according to whether the viruses were detected by on-access scanning or an on-demand scan, as explained below.

### On-access scanning

If on-access scanning detects a virus, Sophos Anti-Virus denies access to the file and by default displays a desktop pop-up alert like the one shown below.



If the desktop pop-up alert cannot be displayed, a command-line alert is displayed instead.

For information about cleaning up viruses, see [Cleaning up viruses](#) (page 16).

### On-demand scans

If an on-demand scan detects a virus, by default Sophos Anti-Virus displays a command-line alert. It reports the virus on the line which starts with >>> followed by either Virus or Virus Fragment:

```
SAVScan virus detection utility
Version 4.50.0 [Linux/Intel]
Virus data version 4.50, February 2010
Includes detection for 1375239 viruses, Trojans and worms
Copyright (c) 1989-2010 Sophos Group. All rights reserved.

System time 13:43:32, System date 02 March 2010

IDE directory is: /opt/sophos-av/lib/sav

Using IDE file nyrate-d.ide
. . . . .
Using IDE file injec-lz.ide

Quick Scanning

>>> Virus 'EICAR-AV-Test' found in file /usr/mydirectory/eicar.src

33 files scanned in 2 seconds.
1 virus was discovered.
1 file out of 33 was infected.
Please send infected samples to Sophos for analysis.
For advice consult www.sophos.com or email support@sophos.com
End of Scan.
```

For information about cleaning up viruses, see [Cleaning up viruses](#) (page 16).

## 6 Cleaning up viruses

### 6.1 Get cleanup information

If viruses are reported, you can get information and cleanup advice from the Sophos website.

To get cleanup information:

1. Go to the security analyses page ([www.sophos.com/security/analyses](http://www.sophos.com/security/analyses)).
2. Search for the analysis of the virus, by using the name that was reported by Sophos Anti-Virus.

### 6.2 Quarantining infected files

You can configure an on-demand scan to put infected files into quarantine to prevent them from being accessed. It does this by changing the ownership and permissions for the files.

**Note:** If you specify disinfection (see [Cleaning up infected files](#) (page 17)) as well as quarantining, Sophos Anti-Virus attempts to disinfect infected items and quarantines them only if disinfection fails.

In this section, where *path* appears in a command, it refers to the path to be scanned.

#### 6.2.1 Specify quarantining

- To specify quarantining, use the option **--quarantine**. Type:  
`savscan path --quarantine`

#### 6.2.2 Specifying the ownership and permissions that are applied

By default, Sophos Anti-Virus changes:

- The user ownership of an infected file to the user running Sophos Anti-Virus.
- The group ownership of the file to the group to which that user belongs.
- The file permissions to `-r-----` (0400).

If you prefer, you can change the user or group ownership and file permissions that Sophos Anti-Virus applies to infected files. You do so by using these parameters:

```
uid=nnn
user=username
gid=nnn
group=group-name
mode=ppp
```



You cannot specify more than one parameter for user ownership or for group ownership. For example, you cannot specify a **uid** and a **user**.

For each parameter that you do not specify, the default setting (as given earlier) is used.

For example:

```
savscan fred --quarantine:user=virus,group=virus,mode=0400
```

changes an infected file's user ownership to "virus", the group ownership to "virus", and the file permissions to `-r-----`. This means that the file is owned by the user "virus" and group "virus", but only the user "virus" can access the file (and only for reading). No-one else (apart from root) can do anything to the file.

You may need to be running as a special user or as superuser to set the ownership and permissions.

## 6.3 Cleaning up infected files

You can configure an on-demand scan to clean up (disinfect or delete) infected files. Any actions that Sophos Anti-Virus takes against infected files are listed in the scan summary and logged in the Sophos Anti-Virus log. By default, cleanup is disabled.

In this section, where *path* appears in a command, it refers to the path to be scanned.

### 6.3.1 Disinfect a specific infected file

- To disinfect a specific infected file, use the option **-di**. Type:  
**savscan path -di**

Sophos Anti-Virus asks for confirmation before it disinfects.

**Note:** Disinfecting an infected document does not repair any changes the virus has made to the document. (See [Get cleanup information](#) (page 16) to find out how to view details on the Sophos website of the virus's side-effects.)

### 6.3.2 Disinfect all infected files on the computer

- To disinfect all infected files on the computer, type:  
**savscan / -di**

Sophos Anti-Virus asks for confirmation before it disinfects.

**Note:** Disinfecting an infected document does not repair any changes the virus has made to the document. (See [Get cleanup information](#) (page 16) to find out how to view details on the Sophos website of the virus's side-effects.)

### 6.3.3 Delete a specific infected file

- To delete a specific infected file, use the option **-remove**. Type:  
**savscan path -remove**

Sophos Anti-Virus asks for confirmation before it deletes.

### 6.3.4 Delete all infected files on the computer

- To delete all infected files on the computer, type:  
**savscan / -remove**

Sophos Anti-Virus asks for confirmation before it deletes.

### 6.3.5 Disinfect an infected boot sector

- To disinfect an infected boot sector, use the disinfection option **-di** and the boot sector option **-bs**. For example, type:  
**savscan -bs=/dev/fd0 -di**

where **/dev/fd0** is the name of the drive that contains the infected boot sector.

Sophos Anti-Virus asks for confirmation before it disinfects.

## 6.4 Recovering from virus side-effects

Recovery from virus infection depends on how the virus infected the computer. Some viruses leave you with no side-effects to deal with; others may have such extreme side-effects that you have to restore a hard disk in order to recover.

Some viruses gradually make minor changes to data. This type of corruption can be hard to detect. It is therefore very important that you read the virus analysis on the Sophos website, and check documents carefully after disinfection.

Sound backups are crucial. If you did not have them before you were infected, start keeping them in case of future infections.

Sometimes you can recover data from disks damaged by a virus. Sophos can supply utilities for repairing the damage caused by some viruses. Contact Sophos technical support for advice: see [Technical support](#) (page 58).

## 7 View the Sophos Anti-Virus log

Sophos Anti-Virus logs details of scanning activity in the Sophos Anti-Virus log and syslog. In addition, virus and error events are logged in the Sophos Anti-Virus log.

### 7.1 CLI

- To view the Sophos Anti-Virus log, use the command **savlog**. This can be used with various options to restrict the output to certain messages and to control the display.

For example, to display all messages logged to the Sophos Anti-Virus log in the last 24 hours, and to display the date and time in UTC/ISO 8601 format, type:

```
/opt/sophos-av/bin/savlog --today --utc
```

- To see a complete list of the options that can be used with **savlog**, type:

```
man savlog
```

### 7.2 Web UI

- To view the Sophos Anti-Virus log, on the **Log Viewer** tab, in the **Log selection** panel, use the text boxes and option buttons to specify the messages that you want to display. Then click **View Log**.

The messages are displayed in the **Log Contents** panel.

## 8 Update Sophos Anti-Virus immediately

Provided that you have enabled auto-updating, Sophos Anti-Virus is kept updated automatically. However, you can also update Sophos Anti-Virus immediately, without waiting for the next automatic update.

- To update Sophos Anti-Virus immediately, at the computer that you want to update, type:  
**`/opt/sophos-av/bin/savupdate`**

**Note:** You can also update computers immediately from Sophos Enterprise Console.

## 9 About kernel support

### 9.1 About support for new kernel releases

When one of the Linux vendors supported by Sophos Anti-Virus releases an update to its Linux kernel, Sophos releases an update to the Sophos kernel interface module (Talpa) to support this. If you apply a Linux kernel update before you apply the matching Talpa update, Sophos Anti-Virus initiates a local compilation of Talpa. If this fails, on-access scanning is stopped and an error is reported.

To avoid this problem, you must confirm that the matching Talpa update has been released before applying the Linux kernel update. A list of supported Linux distributions and updates is available in Sophos support knowledgebase article 14377

(<http://www.sophos.com/support/knowledgebase/article/14377.html>). When the required Talpa update is listed, it is available for download. Provided that you have enabled auto-updating, Sophos Anti-Virus downloads the update automatically. Alternatively, to update Sophos Anti-Virus immediately, without waiting for the next automatic update, type:

**`/opt/sophos-av/bin/savupdate`**

You can then apply the Linux kernel update.

### 9.2 About support for customized kernels

If you customize your Linux kernels, this manual does not explain how to configure updating to support this. See Sophos support knowledgebase article 13503

(<http://www.sophos.com/support/knowledgebase/article/13503.html>).

## 10 Configure the web UI

**Note:** If you are configuring a single computer that is on a network, the configuration might be overwritten if the computer downloads a new CID-based configuration.

To configure the web UI:

1. At the computer that is running the web UI, type:  
**/opt/sophos-av/bin/savsetup**

**savsetup** asks you to select what you want to do.

2. Select **Sophos Anti-Virus GUI configuration**.

**savsetup** asks you a series of questions about the web UI. Type your responses to configure the web UI.

## 11 Appendix A: On-demand scan return codes

**savscan** returns a code to the shell that indicates the result of the scan. You can view the code by entering a further command after the scan has finished, for example:

**echo \$?**

| Return code | Description   |
|-------------|---|
| 0           | No errors occur and no viruses are detected               |
| 1           | The user interrupts the scan by pressing CTRL+C           |
| 2           | An error occurs that prevents further execution of a scan |
| 3           | A virus is detected                                       |

### 11.1 Extended return codes

**savscan** returns a more detailed code to the shell if you run it with the **-eec** option. You can view the code by entering a further command after the scan has finished, for example:

**echo \$?**

| Extended return code | Description   |
|----------------------|---|
| 0                    | No errors occur and no viruses are detected             |
| 8                    | A survivable error occurs                               |
| 16                   | A password-protected file is found (it is not scanned)  |
| 20                   | An item containing a virus is detected and disinfected  |
| 24                   | An item containing a virus is found and not disinfected |
| 28                   | A virus is detected in memory                           |
| 32                   | An integrity check failure occurs                       |

| Extended return code | Description                  |
|----------------------|------------------------------|
| 36                   | An unsurvivable error occurs |
| 40                   | The scan is interrupted      |



## 12 Appendix B: About CID-based configuration

Central installation directory (CID)-based configuration is an alternative to configuration from Sophos Enterprise Console. You can use it to configure all features except on-demand scans, for which you should see [Configuring on-demand scans](#) (page 11).

**Note:** Do not use CID-based configuration unless technical support advises you to do so, or you cannot use Enterprise Console. You cannot use Enterprise Console configuration and CID-based configuration together.

CID-based configuration does not require a Windows computer. It involves making changes to a configuration file that is stored in the CID, by setting the values of parameters using the command **savconfig** (see [savconfig configuration command](#) (page 28)). Then, when computers update from the CID, they use this configuration.

You can also lock any parameters so that they cannot be modified on client computers. In this way, you can determine the configuration of Sophos Anti-Virus on each computer, without fear that the settings will be changed by the user of that computer.

There are two configuration files: the *live* configuration file in the CID and the *offline* configuration file stored elsewhere. When you want to change the live file, you change the offline file, and replace the live file with the offline file. This is explained in the following sections.

## 12.1 Create a CID-based configuration

1. Use the command **savconfig** to set the value of each parameter that you want to set in the offline configuration file.

Use the following syntax:

```
/opt/sophos-av/bin/savconfig -f config-file -c operation parameter value
```

where:

- **-f** specifies that the setting is to be applied to the offline file.
- *config-file* is the path of the offline file, which can be in any directory other than the CID. **savconfig** creates the file for you.
- **-c** indicates that you want to access the Corporate layer of the offline file (for more information about layers, see [About configuration layers](#) (page 28)).
- *operation* is either **set**, **update**, **add**, **remove**, or **delete**.
- *parameter* is the parameter that you want to set.
- *value* is the value to which you want to set the parameter.

For example, to create a file called CIDconfig.cfg in the directory ./config and to disable email alerts, type:

```
/opt/sophos-av/bin/savconfig -f ./config/CIDconfig.cfg -c set EmailNotifier Disabled
```

For information about using **savconfig**, see [savconfig configuration command](#) (page 28).

2. To view the parameter values, use the **query** operation. You can view the value of an individual parameter or all parameters. For example, to view the values of all the parameters that you have set, type:

```
/opt/sophos-av/bin/savconfig -f ./config/CIDconfig.cfg -c query
```

3. When you have finished setting parameters, run the command **addcfg** with the option **-f** and the path of the offline configuration file:

```
/opt/sophos-av/update/cache/Primary/addcfg.sh -f config-file
```

The new configuration is now available for computers to download the next time that they update.

## 12.2 Update a CID-based configuration

1. Use the command **savconfig** to set the value of each parameter that you want to set in the offline configuration file.

Use the following syntax:

```
/opt/sophos-av/bin/savconfig -f config-file -c operation parameter value
```

where:

- **-f** specifies that the setting is to be applied to the offline file.
- *config-file* is the path of the offline file.
- **-c** indicates that you want to access the Corporate layer of the offline file (for more information about layers, see [About configuration layers](#) (page 28)).
- *operation* is either **set**, **update**, **add**, **remove**, or **delete**.
- *parameter* is the parameter that you want to set.
- *value* is the value to which you want to set the parameter.

For example, to update a file called CIDconfig.cfg in the directory ./config and to disable email alerts, type:

```
/opt/sophos-av/bin/savconfig -f ./config/CIDconfig.cfg -c set EmailNotifier Disabled
```

**Note:** You must set *all* the parameters that you want to retain in the Corporate layer of the live file, not just those that you want to update. To use a copy of the current live configuration file as the offline file, copy CorporateLayer.cfg to any directory other than the CID. CorporateLayer.cfg is in the directory config in the CID.

For information about using **savconfig**, see [savconfig configuration command](#) (page 28).

2. To view the parameter values, use the **query** operation. You can view the value of an individual parameter or all parameters. For example, to view the values of all the parameters that you have set, type:

```
/opt/sophos-av/bin/savconfig -f ./config/CIDconfig.cfg -c query
```

3. When you have finished setting parameters, run the command **addcfg** with the option **-f** and the path of the offline configuration file:

```
/opt/sophos-av/update/cache/Primary/addcfg.sh -f config-file
```

The new configuration is now available for computers to download the next time that they update.

## 12.3 About configuration layers

Each installation of Sophos Anti-Virus includes a local configuration file, which includes settings for all features of Sophos Anti-Virus apart from on-demand scans.

Each local configuration file contains a number of layers:

- **Sophos:** This is always present in the file. It includes the factory settings, which are changed only by Sophos.
- **Corporate:** This is present if the installation is configured from the CID.
- **User:** This is present if any local configuration is performed. It includes settings that apply only to the installation on this computer.

Each layer uses the same parameters, so that the same parameter can be set in more than one layer. However, when Sophos Anti-Virus checks the value of a parameter, it does so according to the layer hierarchy:

- By default, Corporate layer overrides User layer.
- Corporate and User layers override Sophos layer.

For example, if a parameter is set in the User layer and the Corporate layer, the value in the Corporate layer is used. Nevertheless, you can unlock the values of individual parameters in the Corporate layer, so that they can be overridden.

When the local configuration file is updated from the configuration file in the CID, the Corporate layer in the local file is replaced by that of the file in the CID.

## 12.4 savconfig configuration command

**savconfig** is the command that you use to configure all features of Sophos Anti-Virus apart from on-demand scanning. The path of the command is `/opt/sophos-av/bin`. Using the command to configure specific functions of Sophos Anti-Virus is explained in the remainder of this manual. The rest of this subsection explains the syntax.

The syntax of **savconfig** is:

**savconfig** [*option*] ... [*operation*] [*parameter*] [*value*] ...

To view a complete list of the options, operations, and parameters, type:

**man savconfig**

### 12.4.1 *option*

You can specify one or more options. The options are mainly associated with the *layers* in the local configuration files in each installation. For information about layers, see [About configuration layers](#)

(page 28). By default, the command accesses the User layer. If you want to access the Corporate layer for example, use the option **-c** or **--corporate**.

By default, the values of parameters in the Corporate layer are locked, so that they override values in the User layer. If you want to allow a corporate setting to be overridden by users, use the option **--nolock**. For example, to set the value of **LogMaxSizeMB** and allow it to be overridden, type:

```
/opt/sophos-av/bin/savconfig --nolock -f corpconfig.cfg -c LogMaxSizeMB 50
```

If you are using Enterprise Console, you can display just the values of the anti-virus policy parameters by using the option **--consoleav**. Type:

```
/opt/sophos-av/bin/savconfig --consoleav query
```

You can display just the values of the Enterprise Console update policy by using the option **--consoleupdate**. Type:

```
/opt/sophos-av/bin/savconfig --consoleupdate query
```

## 12.4.2 operation

You can specify one operation. The operations are mainly associated with how you want to access a parameter. Some parameters can have only one value but others can have a list of values. The operations enable you to add values to a list or remove values from a list. For example, the **Email** parameter is a *list* of email recipients.

To display the values of parameters, use the operation **query**. For example, to display the value of the **EmailNotifier** parameter, type:

```
/opt/sophos-av/bin/savconfig query EmailNotifier
```

If you are using Enterprise Console, when **savconfig** returns values of parameters, those that conflict with the relevant Enterprise Console policy are clearly marked with the word “Conflict”.

## 12.4.3 parameter

You can specify one parameter. To list all the basic parameters that can be set, type:

```
/opt/sophos-av/bin/savconfig -v
```

Some parameters require secondary parameters to be specified as well.

## 12.4.4 value

You can specify one or more values that will be assigned to a parameter. If a value contains spaces, you must enclose it in single quotation marks.

## 13 Appendix C: Configuring scheduled scans

Sophos Anti-Virus can store definitions of one or more scheduled scans.

**Note:** You can also use Enterprise Console or the command **crontab** to scan computers at set times. For details, see the Enterprise Console Help or [Sophos support knowledgebase article 12176](#), respectively. Scheduled scans that have been added using Enterprise Console have names that are prefixed with “SEC:” and cannot be updated or removed except by using Enterprise Console.

### 13.1 Add a scheduled scan from a file

1. To use a template scan definition as a starting point, open `/opt/sophos-av/doc/namedscan.example.en`.  
To create a scan definition from scratch, open a new text file.
2. Define what to scan, when to scan it, and any other options, using only the parameters listed in the template.  
To schedule the scan, you must include at least one day and one time.
3. Save the file in a location of your choosing, being careful not to overwrite the template.
4. Add the scheduled scan to Sophos Anti-Virus using the command **savconfig** with the operation **add** and the parameter **NamedScans**. Specify the name of the scan and the path of the scan definition file.

For example, to add the scan Daily, which is stored in `/home/fred/DailyScan`, type:

```
/opt/sophos-av/bin/savconfig add NamedScans Daily /home/fred/DailyScan
```

### 13.2 Add a scheduled scan from standard input

1. Add the scheduled scan to Sophos Anti-Virus using the command **savconfig** with the operation **add** and the parameter **NamedScans**. Specify the name of the scan and use a hyphen to specify that the definition is to be read from standard input.

For example, to add the scan Daily, type:

```
/opt/sophos-av/bin/savconfig add NamedScans Daily -
```

When you press ENTER, Sophos Anti-Virus waits for you to type the definition of the scheduled scan.

2. Define what to scan, when to scan it, and any other options, using only the parameters listed in the template scan definition: `/opt/sophos-av/doc/namedscan.example.en`. After typing each parameter and its value, press ENTER.  
To schedule the scan, you must include at least one day and one time.
3. To complete the definition, press CTRL+D.

## 13.3 Export a scheduled scan to a file

- To export a scheduled scan from Sophos Anti-Virus to a file, use the command **savconfig** with the operation **query** and the parameter **NamedScans**. Specify the name of the scan and the path of the file to which you want to export the scan.

For example, to export the scan Daily to the file /home/fred/DailyScan, type:

```
/opt/sophos-av/bin/savconfig query NamedScans Daily > /home/fred/DailyScan
```

## 13.4 Export names of all scheduled scans to a file

- To export the names of all scheduled scans (including those that have been created using Enterprise Console) from Sophos Anti-Virus to a file, use the command **savconfig** with the operation **query** and the parameter **NamedScans**. Specify the path of the file to which you want to export the scan names.

For example, to export the names of all scheduled scans to the file /home/fred/AllScans, type:

```
/opt/sophos-av/bin/savconfig query NamedScans > /home/fred/AllScans
```

**Note:** SEC:FullSystemScan is a scan that is always defined if the computer is managed by Enterprise Console.

## 13.5 Export a scheduled scan to standard output

- To export a scheduled scan from Sophos Anti-Virus to standard output, use the command **savconfig** with the operation **query** and the parameter **NamedScans**. Specify the name of the scan.

For example, to export the scan Daily to standard output, type:

```
/opt/sophos-av/bin/savconfig query NamedScans Daily
```

## 13.6 Export names of all scheduled scans to standard output

- To export the names of all scheduled scans (including those that have been created using Enterprise Console) from Sophos Anti-Virus to standard output, use the command **savconfig** with the operation **query** and the parameter **NamedScans**.

For example, to export the names of all scheduled scans to standard output, type:

```
/opt/sophos-av/bin/savconfig query NamedScans
```

**Note:** SEC:FullSystemScan is a scan that is always defined if the computer is managed by Enterprise Console.

## 13.7 Update a scheduled scan from a file

**Note:** You cannot update scheduled scans that have been added using Enterprise Console.

1. Open the file that defines the scheduled scan that you want to update.  
If the scan is not already defined in a file, you can export the scan to a file, as explained in [Export a scheduled scan to a file](#) (page 31).
2. Amend the definition as necessary, using only the parameters listed in the template scan definition: `/opt/sophos-av/doc/namedscan.example.en`. You must define the scan completely, instead of just specifying what you want to update.
3. Save the file.
4. Update the scheduled scan in Sophos Anti-Virus using the command **savconfig** with the operation **update** and the parameter **NamedScans**. Specify the name of the scan and the path of the scan definition file.

For example, to update the scan Daily, which is stored in `/home/fred/DailyScan`, type:

```
/opt/sophos-av/bin/savconfig update NamedScans Daily /home/fred/DailyScan
```

## 13.8 Update a scheduled scan from standard input

**Note:** You cannot update scheduled scans that have been added using Enterprise Console.

1. Update the scheduled scan in Sophos Anti-Virus using the command **savconfig** with the operation **update** and the parameter **NamedScans**. Specify the name of the scan and use a hyphen to specify that the definition is to be read from standard input.

For example, to update the scan Daily, type:

```
/opt/sophos-av/bin/savconfig update NamedScans Daily -
```

When you press ENTER, Sophos Anti-Virus waits for you to type the definition of the scheduled scan.

2. Define what to scan, when to scan it, and any other options, using only the parameters listed in the template scan definition: `/opt/sophos-av/doc/namedscan.example.en`. After typing each parameter and its value, press ENTER. You must define the scan completely, instead of just specifying what you want to update.

To schedule the scan, you must include at least one day and one time.

3. To complete the definition, press CTRL+D.

## 13.9 Remove a scheduled scan

**Note:** You cannot remove scheduled scans that have been added using Enterprise Console.



- To remove a scheduled scan from Sophos Anti-Virus, use the command **savconfig** with the operation **remove** and the parameter **NamedScans**. Specify the name of the scan.

For example, to remove the scan Daily, type:

```
/opt/sophos-av/bin/savconfig remove NamedScans Daily
```

## 13.10 Remove all scheduled scans

**Note:** You cannot remove scheduled scans that have been added using Enterprise Console.

- To remove all scheduled scans from Sophos Anti-Virus, type:  

```
/opt/sophos-av/bin/savconfig delete NamedScans
```

## 14 Appendix D: Configuring alerts

**Note:** If you are configuring a single computer that is on a network, the configuration might be overwritten if the computer downloads a new console-based or CID-based configuration.

You can configure Sophos Anti-Virus to send an alert when it detects viruses, there is a scanning error, or some other type of error. Alerts can be sent via the following methods:

- Desktop pop-ups (on-access scanning only)
- Command-line (on-access scanning only)
- Email (on-access and on-demand scanning)

Desktop pop-up and command-line alerts are sent in the language of the computer that raises the alert. Email alerts can be sent in English or Japanese.

### 14.1 Configuring desktop pop-up alerts

#### 14.1.1 Turn off desktop pop-up alerts

By default, desktop pop-up alerts are turned on.

##### 14.1.1.1 CLI

- To turn off desktop pop-up alerts, type:  
`/opt/sophos-av/bin/savconfig set UIpopupNotification disabled`
- To turn off both desktop pop-up and command-line alerts, type:  
`/opt/sophos-av/bin/savconfig set UINotifier disabled`

##### 14.1.1.2 Web UI

- To turn off desktop pop-up alerts, on the **Alerts** tab, in the **Desktop Pop-up and Command-line** panel, clear the **Enable desktop pop-up alerts** check box. Click **Set** to apply the change.

#### 14.1.2 Specify custom message

A custom English message is included in each desktop pop-up alert in addition to the alert message itself. You can change the text of this custom message but it is not translated. The same message is used for command-line alerts.

##### 14.1.2.1 CLI

- To specify the custom message, use the parameter **UIContactMessage**. For example, type:  
`/opt/sophos-av/bin/savconfig set UIContactMessage 'Contact IT'`

### 14.1.2.2 Web UI

- To specify the custom message, on the **Alerts** tab, in the **Desktop Pop-up and Command-line** panel, type the message in the **Additional message** text box. Click **Set** to apply the change.

## 14.2 Configuring command-line alerts

### 14.2.1 Turn off command-line alerts

By default, command-line alerts are turned on.

#### 14.2.1.1 CLI

- To turn off command-line alerts, type:  
`/opt/sophos-av/bin/savconfig set UIttyNotification disabled`
- To turn off both desktop pop-up and command-line alerts, type:  
`/opt/sophos-av/bin/savconfig set UINotifier disabled`

#### 14.2.1.2 Web UI

- To turn off command-line alerts, on the **Alerts** tab, in the **Desktop Pop-up and Command-line** panel, clear the **Enable command-line alerts** check box. Click **Set** to apply the change.

### 14.2.2 Specify custom message

A custom English message is included in each command-line alert in addition to the alert message itself. You can change the text of this custom message but it is not translated. The same message is used for desktop pop-up alerts.

#### 14.2.2.1 CLI

- To specify the custom message, use the parameter **UIContactMessage**. For example, type:  
`/opt/sophos-av/bin/savconfig set UIContactMessage 'Contact IT'`

#### 14.2.2.2 Web UI

- To specify the custom message, on the **Alerts** tab, in the **Desktop Pop-up and Command-line** panel, type the message in the **Additional message** text box. Click **Set** to apply the change.

## 14.3 Configuring email alerts

### 14.3.1 Turn off email alerts

By default, email alerts are turned on.

#### 14.3.1.1 CLI

- To turn off email alerts, type:  
`/opt/sophos-av/bin/savconfig set EmailNotifier disabled`

#### 14.3.1.2 Web UI

- To turn off email alerts, on the **Alerts** tab, in the **Email** panel, clear the **Enable email alerts** check box. Click **Set** to apply the change.

### 14.3.2 Specify the SMTP server hostname or IP address

By default, the hostname and port of the SMTP server are localhost:25.

#### 14.3.2.1 CLI

- To specify the hostname or IP address of the SMTP server, use the parameter **EmailServer**. For example, type:  
`/opt/sophos-av/bin/savconfig set EmailServer 171.17.31.184`

#### 14.3.2.2 Web UI

- To specify the hostname or IP address of the SMTP server, on the **Alerts** tab, in the **Email** panel, type the hostname or IP address in the **Hostname or IP address of the SMTP server** text box. Click **Set** to apply the change.

### 14.3.3 Specify the language

By default, the language that is used for the alert message itself is English.

#### 14.3.3.1 CLI

- To specify the language that is used for the alert message itself, use the parameter **EmailLanguage**. Currently, valid values are just **English** or **Japanese**. For example, type:  
`/opt/sophos-av/bin/savconfig set EmailLanguage Japanese`

**Note:** This language selection applies only to the alert message itself, not the custom message that is included in each email alert in addition to the alert message itself.

### 14.3.3.2 Web UI

- To specify the language that is used for the alert message itself, on the **Alerts** tab, in the **Email** panel, click the language in the **Language to use in notification emails** list. Click **Set** to apply the change.

**Note:** This language selection applies only to the alert message itself, not the custom message that is included in each email alert in addition to the alert message itself.

## 14.3.4 Specify the email recipients

By default, email alerts are sent to root@localhost.

### 14.3.4.1 CLI

- To add an address to the list of recipients of email alerts, use the parameter **Email** with the operation **add**. For example, type:  
`/opt/sophos-av/bin/savconfig add Email admin@localhost`

**Note:** You can specify more than one recipient in the same command. Separate each recipient by using a space.

- To remove an address from the list, use the parameter **Email** with the operation **remove**. For example, type:  
`/opt/sophos-av/bin/savconfig remove Email admin@localhost`

### 14.3.4.2 Web UI

- To add an address to the list of recipients of email alerts, on the **Alerts** tab, in the **Email** panel, type the address in the **Email recipients** text box. Click **Add New Entry** to add the address to the list of recipients.
- To remove an address from the list, click the address and click **Remove Selected Entry**.

## 14.3.5 Specify what happens if viruses are detected on access

By default, Sophos Anti-Virus sends an email alert if on-access scanning detects viruses. A custom English message is included in each alert in addition to the alert message itself. You can change the text of this custom message but it is not translated.

### 14.3.5.1 CLI

- To turn off the sending of email alerts if viruses are detected on access, type:  
`/opt/sophos-av/bin/savconfig set SendThreatEmail disabled`
- To specify the custom message, use the parameter **ThreatMessage**. For example, type:  
`/opt/sophos-av/bin/savconfig set ThreatMessage 'Contact IT'`

#### 14.3.5.2 Web UI

- To turn off the sending of email alerts if viruses are detected on access, on the **Alerts** tab, in the **Email** panel, clear the **Send email when virus detected** check box. Click **Set** to apply the change.
- To specify the custom message, on the **Alerts** tab, in the **Email** panel, type the message in the **Additional message to be included in virus detection email alerts** text box. Click **Set** to apply the change.

### 14.3.6 Specify what happens if there is an on-access scanning error

By default, Sophos Anti-Virus sends an email alert if there is an on-access scanning error. A custom English message is included in each alert in addition to the alert message itself. You can change the text of this custom message but it is not translated.

#### 14.3.6.1 CLI

- To turn off the sending of email alerts if there is an on-access scanning error, type:  
`/opt/sophos-av/bin/savconfig set SendErrorEmail disabled`
- To specify the custom message, use the parameter **ScanErrorMessage**. For example, type:  
`/opt/sophos-av/bin/savconfig set ScanErrorMessage 'Contact IT'`

#### 14.3.6.2 Web UI

- To turn off the sending of email alerts if there is an on-access scanning error, on the **Alerts** tab, in the **Email** panel, clear the **Send email when there is a scan error** check box. Click **Set** to apply the change.
- To specify the custom message, on the **Alerts** tab, in the **Email** panel, type the message in the **Additional message to be included in scan error email alerts** text box. Click **Set** to apply the change.

### 14.3.7 Turn on-demand email alerts off

By default, Sophos Anti-Virus emails the summary of an on-demand scan if, and only if, the scan detects viruses.

- To turn off the emailing of an on-demand scan summary if viruses are detected, type:  
`/opt/sophos-av/bin/savconfig set EmailDemandSummaryIfThreat disabled`

## 14.3.8 Specify what happens if an event is logged

By default, Sophos Anti-Virus sends an email alert when an event is logged in the Sophos Anti-Virus log. A custom English message is included in each alert in addition to the alert message itself. You can change the text of this custom message but it is not translated.

### 14.3.8.1 CLI

- To specify the custom message, use the parameter **LogMessage**. For example, type:  
`/opt/sophos-av/bin/savconfig set LogMessage 'Contact IT'`

### 14.3.8.2 Web UI

- To specify the custom message, on the **Alerts** tab, in the **Email** panel, type the message in the **Additional message to be included in log event email alerts** text box. Click **Set** to apply the change.

## 15 Appendix E: Configure logging

**Note:** If you are configuring a single computer that is on a network, the configuration might be overwritten if the computer downloads a new console-based or CID-based configuration.

By default, scanning activity is logged in the Sophos Anti-Virus log: `/opt/sophos-av/log/savd.log`. When it reaches 1 MB in size, it is backed up to the same directory automatically and a new log is started.

- To see the default number of logs that are kept, type:  
`/opt/sophos-av/bin/savconfig -s query LogMaxSizeMB`
- To specify the maximum number of logs that are kept, use the parameter **LogMaxSizeMB**. For example, to set the maximum number of logs to 50, type:  
`/opt/sophos-av/bin/savconfig set LogMaxSizeMB 50`



## 16 Appendix F: Configuring updating

**Important:** If you manage Sophos Anti-Virus using Sophos Enterprise Console, you must configure updating using Enterprise Console. For information about how to do this, see the Enterprise Console Help instead of this section.

### 16.1 Basic concepts

#### Update server

An *update server* is a computer on which you have installed Sophos Anti-Virus and which also acts as an update source for other computers. These other computers are either update servers or update clients, depending on how you deploy Sophos Anti-Virus across the network.

#### Update client

An *update client* is a computer on which you have installed Sophos Anti-Virus and which does not need to act as an update source for other computers.

#### Primary update source

The *primary update source* is the location of the updates that a computer usually accesses. It might need access credentials.

#### Secondary update source

The *secondary update source* is the location of the updates that a computer accesses when the primary update source is unavailable. It might need access credentials.

### 16.2 savsetup configuration command

**savsetup** is a command that you can use to configure updating. You should use it only for the specific tasks explained in the following subsections.

Although it enables you to access only some of the parameters that you can access with **savconfig**, it is easier to use. It prompts you for values of parameters, and you respond by selecting or typing the values. To run **savsetup**, type:

```
/opt/sophos-av/bin/savsetup
```

### 16.3 Check the auto-updating configuration for a computer

1. At the computer that you want to check, type:  

```
/opt/sophos-av/bin/savsetup
```

  
**savsetup** asks you to select what you want to do.
2. Select **Auto-updating configuration**.  
  
**savsetup** asks you to select what you want to do.

3. Select **Display update configuration** to see the current configuration.

## 16.4 Configure the update server to update from Sophos directly

1. At the update server, type:  
`/opt/sophos-av/bin/savsetup`  
`savsetup` asks you to select what you want to do.
2. Select **Auto-updating configuration**.  
`savsetup` asks you to select what you want to do.
3. Select the option to configure the primary update source to be Sophos.  
`savsetup` prompts you for credentials.
4. Enter the username and password that are included with your license.  
`savsetup` asks you if you need a proxy to access Sophos.
5. If you need a proxy, press Y and then type the proxy details.

## 16.5 Configure multiple update clients to update from the update server

**Note:** If you want to change the configuration for a single update client, see [Configure a single update client to update from the update server](#) (page 44) instead.

At the update server, you update the offline configuration file, and then apply the changes to the live configuration file, ready for the update clients to download the next time that they update. In the procedure below, *config-file* represents the path of the offline configuration file.

To configure multiple update clients to update from the update server:

1. Set the primary update source address to the location of the CID, using the parameter **PrimaryUpdateSourcePath**. You can specify either an HTTP address or a UNC path, depending on how you have set up the update server. For example, type:  
`/opt/sophos-av/bin/savconfig -f config-file -c set PrimaryUpdateSourcePath 'http://www.mywebcid.com/cid'`
2. If the primary update source requires authentication, set the username and password using the parameters **PrimaryUpdateUsername** and **PrimaryUpdatePassword**, respectively. For example, type:  
`/opt/sophos-av/bin/savconfig -f config-file -c set PrimaryUpdateUsername 'fred'`  
`/opt/sophos-av/bin/savconfig -f config-file -c set PrimaryUpdatePassword 'j23rjfwj'`

3. If you access the primary update source via a proxy, set the address, username, and password of the proxy server, using the parameters **PrimaryUpdateProxyAddress**, **PrimaryUpdateProxyUsername**, and **PrimaryUpdateProxyPassword**, respectively. For example, type:
 

```
/opt/sophos-av/bin/savconfig -f config-file -c set PrimaryUpdateProxyAddress 'http://www-cache.xyz.com:8080'
```

```
/opt/sophos-av/bin/savconfig -f config-file -c set PrimaryUpdateProxyUsername 'penelope'
```

```
/opt/sophos-av/bin/savconfig -f config-file -c set PrimaryUpdateProxyPassword 'fj202jrjf'
```
4. When you have finished setting parameters, run the command **addcfg** with the option **-f** and the path of the offline configuration file:
 

```
/opt/sophos-av/update/cache/Primary/addcfg.sh -f config-file
```

The new configuration is now available for computers to download the next time that they update.

## 16.6 Configure multiple update clients to update from Sophos directly when the update server is unavailable

**Note:** If you want to change the configuration for a single update client, see [Configure a single update client to update from Sophos directly](#) (page 45) instead.

At the update server, you update the offline configuration file, and then apply the changes to the live configuration file, ready for the update clients to download the next time that they update. In the procedure below, *config-file* represents the path of the offline configuration file.

To configure multiple update clients to update from Sophos directly when the update server is unavailable:

1. Set the secondary update source address to **sophos:**, using the parameter **SecondaryUpdateSourcePath**. For example, type:
 

```
/opt/sophos-av/bin/savconfig -f config-file -c set SecondaryUpdateSourcePath 'sophos:'
```
2. Set the secondary update source username to the username that is included with your license, using the parameter **SecondaryUpdateUsername**. For example, type:
 

```
/opt/sophos-av/bin/savconfig -f config-file -c set SecondaryUpdateUsername 'cust123'
```
3. Set the secondary update source password to the password that is included with your license, using the parameter **SecondaryUpdatePassword**. For example, type:
 

```
/opt/sophos-av/bin/savconfig -f config-file -c set SecondaryUpdatePassword 'j23rjfwj'
```

4. If you access the internet via a proxy, set the address, username, and password of the proxy server, using the parameters **SecondaryUpdateProxyAddress**, **SecondaryUpdateProxyUsername**, and **SecondaryUpdateProxyPassword**, respectively. For example, type:  

```
/opt/sophos-av/bin/savconfig -f config-file -c set SecondaryUpdateProxyAddress 'http://www-cache.xyz.com:8080'
```

```
/opt/sophos-av/bin/savconfig -f config-file -c set SecondaryUpdateProxyUsername 'penelope'
```

```
/opt/sophos-av/bin/savconfig -f config-file -c set SecondaryUpdateProxyPassword 'fj202jrjf'
```
5. When you have finished setting parameters, run the command **addcfg** with the option **-f** and the path of the offline configuration file:  

```
/opt/sophos-av/update/cache/Primary/addcfg.sh -f config-file
```

The new configuration is now available for computers to download the next time that they update.

## 16.7 Configure a single update client to update from the update server

**Note:** If you want to change the configuration for multiple update clients, see [Configure multiple update clients to update from the update server](#) (page 42) instead.

To configure a single update client to update from the update server:

1. At the computer that you want to configure, type:  

```
/opt/sophos-av/bin/savsetup
```

**savsetup** asks you to select what you want to do.
2. Select **Auto-updating configuration**.  
**savsetup** asks you to select what you want to do.
3. Select the option to configure the primary (or secondary) update source to be your own server.  
**savsetup** prompts you for details of the update source.
4. Enter the address of the source, and the username and password if required.  
You can specify either an HTTP address or a UNC path, depending on how you have set up the update server.  
**savsetup** asks you if you need a proxy to access the update server.
5. If you need a proxy, press Y and then type the proxy details.

## 16.8 Configure a single update client to update from Sophos directly

**Note:** If you want to change the configuration for multiple update clients, see [Configure multiple update clients to update from Sophos directly when the update server is unavailable](#) (page 43) instead.

To configure a single update client to update from Sophos directly:

1. At the computer that you want to configure, type:  
**/opt/sophos-av/bin/savsetup**  
**savsetup** asks you to select what you want to do.
2. Select **Auto-updating configuration**.  
**savsetup** asks you to select what you want to do.
3. Select the option to configure the primary (or secondary) update source to be Sophos.  
**savsetup** prompts you for credentials.
4. Enter the username and password that are included with your license.  
**savsetup** asks you if you need a proxy to access Sophos.
5. If you need a proxy, press Y and then type the proxy details.

## 17 Appendix G: Configuring on-access scanning

**Note:** If you are configuring a single computer that is on a network, the configuration might be overwritten if the computer downloads a new console-based or CID-based configuration.

### 17.1 Excluding files and directories from scanning

You can exclude files and directories from scanning in two ways:

- Using file or directory name
- Using wildcards

If you want to exclude files and directories whose names are encoded using non-UTF-8, see [Specifying character encoding of directory names and filenames](#) (page 47).

#### 17.1.1 Use file or directory name

**Note:** If you are configuring a single computer that is on a network, the configuration might be overwritten if the computer downloads a new console-based or CID-based configuration.

##### 17.1.1.1 CLI

- To exclude a particular file or directory, use the **ExcludeFilePaths** parameter with the **add** operation. For example, to add the file `/tmp/report` to the list of files and directories to exclude, type:  
`/opt/sophos-av/bin/savconfig add ExcludeFilePaths /tmp/report`
- To remove an exclusion from the list, use the **ExcludeFilePaths** parameter with the **remove** operation. For example, type:  
`/opt/sophos-av/bin/savconfig remove ExcludeFilePaths /tmp/report`

##### 17.1.1.2 Web UI

- To exclude a particular file or directory, on the **Exclusions** tab, in the **File Scanning Exclusions** panel, type the path in the text box labeled **Files or directories (with or without wildcards)**. Click **Add New Entry** to add the path to the list of files and directories to exclude.
- To remove an exclusion from the list, click the exclusion and click **Remove Selected Entry**.

#### 17.1.2 Use wildcards

**Note:** If you are configuring a single computer that is on a network, the configuration might be overwritten if the computer downloads a new console-based or CID-based configuration.

### 17.1.2.1 CLI

- To exclude files and directories by using wildcards, use the **ExcludeFileOnGlob** parameter with the **add** operation. Valid wildcards are **\*** which matches any number of any characters, and **?** which matches any one character. For example, to add all text files in the **/tmp** directory to the list of files and directories to exclude, type:  
`/opt/sophos-av/bin/savconfig add ExcludeFileOnGlob '/tmp/*.txt'`
- If you do not enclose the expression in quotation marks, Linux expands the expression and passes the list of files to Sophos Anti-Virus. This is useful for excluding only files that exist already, and enabling files that are created later to be scanned. For example, to add just text files that exist already in the **/tmp** directory to the list of files and directories to exclude, type:  
`/opt/sophos-av/bin/savconfig add ExcludeFileOnGlob /tmp/*.txt`
- To remove an exclusion from the list, use the **ExcludeFileOnGlob** parameter with the **remove** operation. For example, type:  
`/opt/sophos-av/bin/savconfig remove ExcludeFileOnGlob '/tmp/notes.txt'`

### 17.1.2.2 Web UI

- To exclude files and directories by using wildcards, on the **Exclusions** tab, in the **File Scanning Exclusions** panel, type the path in the text box labeled **Files or directories (with or without wildcards)**. Valid wildcards are **\*** which matches any number of any characters, and **?** which matches any one character. Click **Add New Entry** to add the path to the list of files and directories to exclude.
- To remove an exclusion from the list, select the exclusion and click **Remove Selected Entry**.

### 17.1.3 Specifying character encoding of directory names and filenames

Linux enables you to name directories and files using any character encoding that you choose (for example, UTF-8, EUC\_jp). However, Sophos Anti-Virus stores exclusions only in UTF-8. Therefore, if you want to exclude directories and files from scanning whose names are encoded using non-UTF-8, you specify the exclusions in UTF-8, and specify the encodings using the **ExclusionEncodings** parameter. Then, the names of any directories or files that you exclude are evaluated in each of the encodings that you specified, and all matching directories and files are excluded. This applies to exclusions that have been specified using the **ExcludeFilePaths** and **ExcludeFileOnGlob** parameters. By default, UTF-8, EUC\_jp, and ISO-8859-1 (Latin-1) are specified.

For example, if you want to exclude directories and files whose names are encoded in EUC\_cn, you specify the names of the directories and files using the **ExcludeFilePaths** and/or the **ExcludeFileOnGlob** parameter. Then, you add EUC\_cn to the list of encodings:

```
/opt/sophos-av/bin/savconfig add ExclusionEncodings EUC_cn
```

Then, Sophos Anti-Virus evaluates in UTF-8, EUC\_jp, ISO-8859-1 (Latin-1), and EUC\_cn all the directory names and filenames that you specified. It then excludes all directories and files whose names match.

## 17.2 Exclude a filesystem type from scanning

By default, no filesystem types are excluded.

### 17.2.1 CLI

- To exclude a filesystem type, use the **ExcludeFilesystems** parameter with the **add** operation. Valid filesystem types are listed in the file **/proc/filesystems**. For example, to add **nfs** to the list of filesystem types to exclude, type:  
`/opt/sophos-av/bin/savconfig add ExcludeFilesystems nfs`
- To remove an exclusion from the list, use the **ExcludeFilesystems** parameter with the **remove** operation. For example, type:  
`/opt/sophos-av/bin/savconfig remove ExcludeFilesystems nfs`

### 17.2.2 Web UI

- To exclude a filesystem type, on the **Exclusions** tab, in the **File Scanning Exclusions** panel, click one of the filesystem types in the **Filesystem types** list. Click **Add New Entry** to add the filesystem type to the list of filesystem types to exclude.
- To remove an exclusion from the list, click the exclusion and click **Remove Selected Entry**.

## 17.3 Scan inside archives

By default, on-access scanning inside archives is turned off. However, you might want to turn on the option if you are dealing with several such files at a time and the cost of not detecting a virus is high. For example, you might be emailing some archives to an important contact.

**Note:** We recommend that you do not turn on this option, for the following reasons:

- Scanning inside archives makes scanning significantly slower.
- Whether you turn on this option or not, when you open a file extracted from an archive, the extracted file is scanned.

### 17.3.1 CLI

- To turn *on* scanning inside archives, type:  
`/opt/sophos-av/bin/savconfig set ScanArchives enabled`



- To turn *off* scanning inside archives, type:  
`/opt/sophos-av/bin/savconfig set ScanArchives disabled`

## 17.3.2 Web UI

- To turn on scanning inside archives, on the **Scanning** tab, in the **Archive Scanning** panel, select the **Scan inside archives** check box. Click **Set** to apply the change.

## 17.4 Cleaning up infected files

You can configure on-access scanning to clean up (disinfect or delete) infected files. Any actions that Sophos Anti-Virus takes against infected files are logged in the Sophos Anti-Virus log. By default, cleanup is disabled.

**Note:** You can turn on both disinfection and deletion, but we do not recommend it. If you do this, Sophos Anti-Virus first tries to disinfect the file. If disinfection fails, it deletes it.

### 17.4.1 Disinfect infected files and boot sectors

#### 17.4.1.1 CLI

- To turn *on* disinfection of infected files and boot sectors on access, type:  
`/opt/sophos-av/bin/savconfig add AutomaticAction disinfect`

**Important:** Sophos Anti-Virus does not ask for confirmation before it disinfects.

**Note:** Disinfecting an infected document does not repair any changes the virus has made to the document. (See [Get cleanup information](#) (page 16) to find out how to view details on the Sophos website of the virus's side-effects.)

- To turn *off* disinfection of infected files and boot sectors on access, type:  
`/opt/sophos-av/bin/savconfig remove AutomaticAction disinfect`

#### 17.4.1.2 Web UI

- To turn on disinfection of infected files and boot sectors on access, on the **Scanning** tab, in the **Cleanup** panel, select the **Automatically disinfect infected items** check box. Click **Set** to apply the change.

**Important:** Sophos Anti-Virus does not ask for confirmation before it disinfects.

**Note:** Disinfecting an infected document does not repair any changes the virus has made to the document. (See [Get cleanup information](#) (page 16) to find out how to view details on the Sophos website of the virus's side-effects.)

## 17.4.2 Delete infected files

**Important:** You should use this option only if advised to by Sophos technical support. If the infected file is a mailbox, Sophos Anti-Virus might delete the whole mailbox.

### 17.4.2.1 CLI

- To turn *on* deletion of infected files on access, type:  
`/opt/sophos-av/bin/savconfig add AutomaticAction delete`

**Important:** Sophos Anti-Virus does not ask for confirmation before it deletes.

- To turn *off* deletion of infected files on access, type:  
`/opt/sophos-av/bin/savconfig remove AutomaticAction delete`

### 17.4.2.2 Web UI

- To turn on deletion of infected files on access, on the **Scanning** tab, in the **Cleanup** panel, select the **Automatically delete infected items** check box. Click **Set** to apply the change.

**Important:** Sophos Anti-Virus does not ask for confirmation before it deletes.

## 18 Troubleshooting

This section describes how to deal with problems that might arise when using Sophos Anti-Virus.

For information about Sophos Anti-Virus return codes for on-demand scans, see [Appendix A: On-demand scan return codes](#) (page 23).

### 18.1 Unable to run a command

#### Symptom

Your computer does not allow you to run a Sophos Anti-Virus command.

#### Cause

This might be because you do not have sufficient privileges.

#### Resolve the problem

Try logging on to the computer as root.

### 18.2 Exclusion configuration has not been applied

#### Symptom

Occasionally, when you configure Sophos Anti-Virus to include files for on-access scanning that were previously excluded, the files remain excluded.

#### Cause

This might be because the cache of files that have previously been scanned still includes the files that were previously excluded.

#### Resolve the problem

Try flushing the cache. Type:

```
echo 'disable' > /proc/sys/talpa/intercept-filters/Cache/status
```

```
echo 'enable' > /proc/sys/talpa/intercept-filters/Cache/status
```

### 18.3 Computer reports “No manual entry for ...”

#### Symptom

When you try to view a Sophos Anti-Virus man page, the computer displays a message similar to No manual entry for ....

### Cause

This is probably because the environment variable MANPATH does not include the path to the man page.

### Resolve the problem

1. If you are running the sh, ksh or bash shell, open /etc/profile for editing.

If you are running the csh or tcsh shell, open /etc/login for editing.

**Note:** If you do not have a login script or profile, carry out the following steps at the command prompt. You must do this every time that you restart the computer.

2. Check that the environment variable MANPATH includes the directory /usr/local/man.
3. If MANPATH does not include this directory, add it as follows. Do not change any of the existing settings.

If you are running the sh, ksh or bash shell, type:

```
MANPATH=$MANPATH:/usr/local/man
```

```
export MANPATH
```

If you are running the csh or tcsh shell, type:

```
setenv MANPATH values:/usr/local/man
```

where *values* are the existing settings.

4. Save the login script or profile.

## 18.4 Sophos Anti-Virus runs out of disk space

### Symptom

Sophos Anti-Virus runs out of disk space, perhaps when scanning complex archives.

### Causes

This might be for one of the following reasons:

- When it unpacks archives, Sophos Anti-Virus uses the /tmp directory to store its working results. If this directory is not very large, Sophos Anti-Virus may run out of disk space.
- Sophos Anti-Virus has exceeded the user's quota.

### Resolve the problem

Try one of the following:

- Enlarge /tmp.
- Increase the user's quota.

- Change the directory that Sophos Anti-Virus uses for working results. You can do this by setting the environment variable SAV\_TMP.

## 18.5 On-demand scanning runs slowly

This problem may arise for one of the following reasons:

### Symptom

Sophos Anti-Virus takes significantly longer to carry out an on-demand scan.

### Causes

This might be for one of the following reasons:

- By default, Sophos Anti-Virus performs a quick scan, which scans only the parts of files that are likely to contain viruses. If scanning is set to full (using the option **-f**), it scans the whole file.
- By default, Sophos Anti-Virus scans only particular file types. If it is configured to scan *all* file types, the process takes longer.

### Resolve the problem

Try one of the following, as appropriate:

- Avoid using full scanning unless you are advised to, for example by Sophos technical support.
- To scan files that have specific filename extensions, add those extensions to the list of file types that Sophos Anti-Virus scans by default. For more information, see [Scan a particular file type](#) (page 11).

## 18.6 Archiver backs up all files that have been scanned on demand

### Symptom

Your archiver always backs up all the files that Sophos Anti-Virus has scanned on demand.

### Cause

This is because of changes that Sophos Anti-Virus makes in the “status-changed” time of files. By default, Sophos Anti-Virus tries to reset the access time (**atime**) of files to the time shown before scanning. However, this has the effect of changing the inode status-changed time (**ctime**). If your archiver uses the **ctime** to decide whether a file has changed, it backs up all files scanned by Sophos Anti-Virus.

### Resolve the problem

Run **savscan** with the option **--no-reset-atime**.

## 18.7 Virus not cleaned up

### Symptoms

- Sophos Anti-Virus has not attempted to clean up a virus.
- Sophos Anti-Virus displays `Disinfection failed`.

### Causes

This might be for one of the following reasons:

- Automatic cleanup has not been enabled.
- Sophos Anti-Virus cannot disinfect that type of virus.
- The infected file is on a removable medium, for example floppy disk or CD, that is write-protected.
- The infected file is on an NTFS filesystem.
- Sophos Anti-Virus does not clean up a virus fragment because it has not found an exact virus match.

### Resolve the problem

Try one of the following, as appropriate:

- Enable automatic cleanup.
- If possible, make the removable medium writeable.
- Deal with files that are on an NTFS filesystem on the local computer instead.

## 18.8 Virus fragment reported

### Symptom

Sophos Anti-Virus reports that it has detected a virus fragment.

### Causes

This indicates that part of a file matches part of a virus. This is for one of the following reasons:

- Many new viruses are based on existing ones. Therefore, code fragments that are typical of a known virus might appear in files that are infected with a new one.
- Many viruses contain bugs in their replication routines that cause them to infect target files incorrectly. An inactive part of the virus (possibly a substantial part) may appear in the host file, and this is detected by Sophos Anti-Virus.
- When running a full scan, Sophos Anti-Virus may report that there is a virus fragment in a database file.

**Resolve the problem**

1. Update Sophos Anti-Virus on the affected computer so that it has the latest virus data.
2. Try to disinfect the file: see [Disinfect a specific infected file](#) (page 17).
3. If virus fragments are still reported, contact Sophos technical support for advice: see [Technical support](#) (page 58).

## 18.9 Connection to web UI refused

**Symptom**

When you try to access the web UI, an error message is displayed that tells you that the connection was refused.

**Cause**

This might be because the web UI daemon is not running.

**Resolve the problem**

Try starting the web UI daemon. Type:

```
/etc/init.d/sav-web start
```

## 18.10 Unable to access disk

**Symptom**

You are unable to access files on a removable disk.

**Cause**

By default, Sophos Anti-Virus prevents access to removable disks whose boot sectors are infected.

**Resolve the problem**

To allow access (for example to copy files from a floppy disk infected with a boot sector virus):

1. Type:  

```
/opt/sophos-av/bin/savconfig set AllowIfBootSectorThreat enabled
```
2. When you have finished accessing the disk, type:  

```
/opt/sophos-av/bin/savconfig set AllowIfBootSectorThreat disabled
```
3. Remove the disk from the computer so that it cannot try to re-infect the computer on restart.

## 19 Glossary

|   |   |
|---|---|
| <b>boot sector virus</b>                    | A type of virus that subverts the initial stages of the booting process. A boot sector virus attacks either the master boot sector or the partition boot sector.  |
| <b>central installation directory (CID)</b> | A directory into which Sophos software and updates are placed. Networked computers update themselves from this directory.   |
| <b>CID</b>                                  | See “central installation directory”.   |
| <b>CID-based configuration</b>              | Such configuration involves making changes to the CID-based configuration file by setting the values of parameters using the command <b>savconfig</b> . When computers update from the CID, they use this configuration. This method was formerly known as “corporate configuration”. |
| <b>disinfection</b>                         | Disinfection removes a virus from a file or boot sector.  |
| <b>on-access scan</b>                       | Your main method of protection against viruses. Whenever you access (copy, save, move, or open) a file, Sophos Anti-Virus scans the file and grants access to it only if it does not pose a threat to your computer.  |
| <b>on-demand scan</b>                       | A scan that you initiate. You can use an on-demand scan to scan anything from a single file to everything on your computer that you have permission to read.  |
| <b>primary update source</b>                | The location of the updates that a computer usually accesses. It might need access credentials.   |
| <b>scheduled scan</b>                       | A scan of your computer, or parts of your computer, that runs at set times.   |
| <b>secondary update source</b>              | The location of the updates that a computer accesses when the primary update source is unavailable. It might need access credentials.   |
| <b>update client</b>                        | A computer on which you have installed Sophos Anti-Virus and which does not need to act as an update source for other computers.  |
| <b>update server</b>                        | A computer on which you have installed Sophos Anti-Virus and which also acts as an update source for other computers. These other   |



computers are either update servers or update clients, depending on how you deploy Sophos Anti-Virus across the network.

**virus**

A computer program that copies itself. Often viruses disrupt computer systems or damage the data contained on them. A virus needs a host program and does not infect a computer until it has been run. Some viruses spread across networks by making copies of themselves or may forward themselves via email. The term “virus” is often also used to refer to viruses, worms, and Trojans.

## 20 Technical support

You can find technical support for Sophos products in any of these ways:

- Visit the SophosTalk community at <http://community.sophos.com/> and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at <http://www.sophos.com/support/>.
- Download the product documentation at <http://www.sophos.com/support/docs/>.
- Send an email to [support@sophos.com](mailto:support@sophos.com), including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

## 21 Legal notices

Copyright © 2005–2011 Sophos Limited. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Limited. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

### **ACE™, TAO™, CIAO™, and CoSMIC™**

ACE<sup>1</sup>, TAO<sup>2</sup>, CIAO<sup>3</sup>, and CoSMIC<sup>4</sup> (henceforth referred to as “DOC software”) are copyrighted by Douglas C. Schmidt<sup>5</sup> and his research group<sup>6</sup> at Washington University<sup>7</sup>, University of California<sup>8</sup>, Irvine, and Vanderbilt University<sup>9</sup>, Copyright © 1993–2005, all rights reserved.

Since DOC software is open-source, free software, you are free to use, modify, copy, and distribute—perpetually and irrevocably—the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using DOC software.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not do anything to the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, that will prevent DOC software from being distributed freely using an open-source development model. You needn’t inform anyone that you’re using DOC software in your software, though we encourage you to let us<sup>10</sup> know so we can promote your project in the DOC software success stories<sup>11</sup>.

DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies<sup>12</sup> around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

The ACE<sup>13</sup>, TAO<sup>14</sup>, CIAO<sup>15</sup>, and CoSMIC<sup>16</sup> web sites are maintained by the DOC Group<sup>17</sup> at the Institute for Software Integrated Systems (ISIS)<sup>18</sup> and the Center for Distributed Object Computing of Washington University, St. Louis<sup>19</sup> for the development of open-source software as part of the open-source software community<sup>20</sup>. By submitting comments, suggestions, code, code snippets,

techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters acknowledge that any such submission might become part of the copyright maintained on the overall body of code, which comprises the DOC software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source DOC software projects or their designees.

The names ACE, TAO, CIAO, CoSMIC, Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. Further, products or services derived from this source may not be called ACE, TAO, CIAO, or CoSMIC nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

If you have any suggestions, additions, comments, or questions, please let me<sup>21</sup> know.

Douglas C. Schmidt<sup>22</sup>

## **References**

1. <http://www.cs.wustl.edu/~schmidt/ACE.html>
2. <http://www.cs.wustl.edu/~schmidt/TAO.html>
3. <http://www.dre.vanderbilt.edu/CIAO/>
4. <http://www.dre.vanderbilt.edu/cosmic/>
5. <http://www.dre.vanderbilt.edu/~schmidt/>
6. <http://www.cs.wustl.edu/~schmidt/ACE-members.html>
7. <http://www.wustl.edu/>
8. <http://www.uci.edu/>
9. <http://www.vanderbilt.edu/>
10. [mailto:doc\\_group@cs.wustl.edu](mailto:doc_group@cs.wustl.edu)
11. <http://www.cs.wustl.edu/~schmidt/ACE-users.html>
12. <http://www.cs.wustl.edu/~schmidt/commercial-support.html>
13. <http://www.cs.wustl.edu/~schmidt/ACE.html>
14. <http://www.cs.wustl.edu/~schmidt/TAO.html>
15. <http://www.dre.vanderbilt.edu/CIAO/>
16. <http://www.dre.vanderbilt.edu/cosmic/>
17. <http://www.dre.vanderbilt.edu/>
18. <http://www.isis.vanderbilt.edu/>
19. <http://www.cs.wustl.edu/~schmidt/doc-center.html>
20. <http://www.opensource.org/>
21. <mailto:d.schmidt@vanderbilt.edu>
22. <http://www.dre.vanderbilt.edu/~schmidt/>

## GNU General Public License

Some software programs are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or similar Free Software licenses which, among other rights, permit the user to copy, modify, and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires for any software licensed under the GPL, which is distributed to a user in an executable binary format, that the source code also be made available to those users. For any such software which is distributed along with this Sophos product, the source code is available by submitting a request to Sophos via email to [savlinuxgpl@sophos.com](mailto:savlinuxgpl@sophos.com). A copy of the GPL terms can be found at [www.gnu.org/copyleft/gpl.html](http://www.gnu.org/copyleft/gpl.html)

## libmagic – file type detection

Copyright © Ian F. Darwin 1986, 1987, 1989, 1990, 1991, 1992, 1994, 1995.

Software written by Ian F. Darwin and others; maintained 1994–2004 Christos Zoulas.

This software is not subject to any export provision of the United States Department of Commerce, and may be exported to any country or planet.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice immediately at the beginning of the file, without modification, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## Medusa web server

Medusa was once distributed under a ‘free for non-commercial use’ license, but in May of 2000 Sam Rushing changed the license to be identical to the standard Python license at the time. The standard Python license has always applied to the core components of Medusa, this change just frees up the rest of the system, including the http server, ftp server, utilities, etc. Medusa is therefore under the following license:

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Sam Rushing not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

SAM RUSHING DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL SAM RUSHING BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Sam would like to take this opportunity to thank all of the folks who supported Medusa over the years by purchasing commercial licenses.

### **OpenSSL cryptographic toolkit**

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

### **OpenSSL license**

Copyright © 1998–2006 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)”

4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

### **Original SSLeay license**

Copyright © 1995–1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape’s SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”

The word “cryptographic” can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

“This product includes software written by Tim Hudson (tjh@cryptsoft.com)”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

### **pycrypto**

Distribute and use freely; there are no restrictions on further dissemination and usage except those imposed by the laws of your country of residence. This software is provided “as is” without warranty of fitness for use or suitability for any purpose, express or implied. Use at your own risk or not at all.

Incorporating the code into commercial products is permitted; you do not have to make source available or contribute your changes back (though that would be nice).

— amk (www.amk.ca)

### **Python**

#### **PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2**

1. This LICENSE AGREEMENT is between the Python Software Foundation (“PSF”), and the Individual or Organization (“Licensee”) accessing and otherwise using this software (“Python”) in source or binary form and its associated documentation.
2. Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, worldwide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python alone or in any derivative version, provided, however, that PSF’s License Agreement and PSF’s notice of copyright, i.e., “Copyright © 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009 Python Software Foundation; All Rights Reserved” are retained in Python alone or in any derivative version prepared by Licensee.
3. In the event Licensee prepares a derivative work that is based on or incorporates Python or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python.



4. PSF is making Python available to Licensee on an “AS IS” basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.
5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.
6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.
7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.
8. By copying, installing or otherwise using Python, Licensee agrees to be bound by the terms and conditions of this License Agreement.

### **TinyXML XML parser**

This software is provided ‘as-is’, without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

### **zlib compression tools**

© 1995–2002 Jean-loup Gailly and Mark Adler

This software is provided ‘as-is’, without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

If you use the zlib library in a product, we would appreciate *\*not\** receiving lengthy legal documents to sign. The sources are provided for free but without warranty of any kind. The library has been entirely written by Jean-loup Gailly and Mark Adler; it does not include third-party code.

If you redistribute modified sources, we would appreciate that you include in the file ChangeLog history information documenting your changes.

# Index

## A

- accessing disks 55
- alerts
  - command-line 14, 35
  - desktop pop-up 14, 34
  - email 36, 39
- analyses of viruses 16
- archives
  - on-access scanning 48
  - on-demand scans 11, 12

## B

- backups of scanned files 53
- boot sectors
  - disinfecting 18
  - infected 55
  - on-demand scans 10

## C

- character encoding 47
- CID-based configuration 6, 25
- cleaning up infected files 17, 49
- cleanup information 16
- CLI (command-line interface) 4
- command-line alerts 14, 35
- command-line interface (CLI) 4
- computer, on-demand scans 10
- configuring Sophos Anti-Virus 6, 25
- customized kernels 21

## D

- deleting infected files 18, 50
- desktop pop-up alerts 14, 34
- directories, on-demand scans 10
- disinfecting
  - boot sectors 18
  - infected files 17
- disk space insufficient 52

- disks, accessing 55

## E

- email alerts 36, 39
- Enterprise Console 6
- error codes 23
- errors, on-access scanning 38
- excluding items
  - character encoding 47
  - on-access scanning 46, 48
  - on-demand scans 13

## F

- file types, on-demand scans 11, 13
- files, on-demand scans 10
- filesystems, on-demand scans 10, 12
- fragment reported, viruses 54

## I

- infected boot sectors 55
- infected files
  - cleaning up 17, 49
  - deleting 18, 50
  - disinfecting 17
  - quarantining 16

## K

- kernels
  - customized 21
  - new releases 21

## L

- layers, in configuration file 28
- log, Sophos Anti-Virus
  - configuring 40
  - viewing 19

## M

- man page not found 51

## **N**

No manual entry for ... 51

## **O**

- on-access scanning 7
  - archives 48
  - errors 38
  - excluding items 46, 48
  - starting 8
  - starting automatically 7
  - status 7
  - stopping 8
- on-demand scans 10
  - archives 11, 12
  - boot sectors 10
  - computer 10
  - directories 10
  - excluding items 13
  - file types 11, 13
  - files 10
  - filesystems 10, 12
  - remote computers 12
  - scheduled scans 30
  - symbolically linked items 12
  - UNIX executables 13

## **Q**

quarantining infected files 16

## **R**

remote computers, on-demand scans 12  
return codes 23

## **S**

savconfig 28  
savsetup 41  
scheduled scans 30  
side-effects of viruses 18  
slow on-demand scans 53  
Sophos Anti-Virus log

- configuring 40
- viewing 19

starting on-access scanning 8  
starting on-access scanning automatically 7  
stopping on-access scanning 8  
symbolically linked items, on-demand scans 12

## **U**

UNIX executables, on-demand scans 13  
updating

- configuring 41
- immediate 20
- support for customized kernels 21
- support for new kernels 21

## **V**

viruses

- analyses 16
- detected 14, 37, 38
- fragment reported 54
- not cleaned up 54
- side-effects 18

## **W**

web UI 5

- configuring 22
- connection problem 55